

Docket No. AUS920000767US1

METHOD AND APPARATUS FOR DYNAMIC MODIFICATION OF INTERNET
FIREWALLS USING VARIABLY-WEIGHTED TEXT RULES

BACKGROUND OF THE INVENTION

5

1. Technical Field:

The present invention relates to Internet access
and, in particular, to content filtering. Still more
particularly, the present invention provides a method,
10 apparatus, and program for dynamic modification of
Internet firewalls using variably-weighted text rules.

2. Description of Related Art:

With the ubiquity of the Internet birthing new
15 business models and ways of working, a variety of risks
are also presented to organizations that seek to
capitalize on the burgeoning e-business trend. Besides
the obvious security risks of damaging or unwarranted
software making its way into an organizational network,
20 liabilities exist, particularly surrounding the download
of indecent or questionable subject matter. In order to
protect both its information infrastructure, as well as
the professional standards expected in a workplace,
companies and non-profits make frequent use of firewalls,
25 the gateways imposed between the internal network and the
outside world, i.e. the Internet.

Firewalls stand at an organization's electronic
connection to the Internet and are routinely configured
to allow or disallow access to sites and services based
30 upon the nature of the services. Firewall configuration
must be performed by an administrator based upon

0033559-11200

Therefore, it would be advantageous to provide a
25 solution to content filtering that does not require human
intervention and manual review of content and does not
impose restrictive and cumbersome desktop filtering best
suited for home computers.

Docket No. AUS920000767US1

SUMMARY OF THE INVENTION

The present invention determines dynamic rules for Internet protocol address which should be inaccessible from an organization. Keywords are entered into a search table. A sliding scale is established, wherein a term may be awarded a point value based upon its severity. Subsequently, a keyword's frequency and point value are used to determine the acceptability of a document source.

10 An organizational policy may be established based upon the total number of points per document served from an Internet protocol address or an average point value for documents served from an Internet protocol address with respect to a threshold. The length of time or number of

15 documents permitted before a decision is reached, namely a decision interval, may be established. A reset policy may be determined to dictate what actions will be taken after the decision interval is reached.

Docket No. AUS920000767US1

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

10 **Figure 1** depicts a pictorial representation of a network of data processing systems in which the present invention may be implemented;

15 **Figure 2** is a block diagram of a data processing system that may be implemented as a server in accordance with a preferred embodiment of the present invention;

Figure 3 is a block diagram illustrating a data processing system in which the present invention may be implemented;

20 **Figure 4** is a block diagram of a firewall host in accordance with a preferred embodiment of the present invention; and

Figure 5 is a flowchart illustrating the operation of a content filtering process in accordance with a preferred embodiment of the present invention.

25

00738589-11200

Docket No. AUS920000767US1

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures, Figure 1 depicts a pictorial representation of a network of data processing systems in which the present invention may be implemented. Network data processing system 100 is a network of computers in which the present invention may be implemented. Network data processing system 100 contains an intranet 102, which is the medium used to provide communications links between various devices and computers connected together within network data processing system 100. Intranet 102 may include connections, such as wire, wireless communication links, or fiber optic cables.

In the depicted example, a server 104 is connected to intranet 102 along with storage unit 106. In addition, clients 108, 110, and 112 also are connected to intranet 102. These clients 108, 110, and 112 may be, for example, personal computers or network computers. In the depicted example, server 104 provides data, such as boot files, operating system images, and applications to clients 108-112. Clients 108, 110, and 112 are clients to server 104.

Network data processing system 100 may include additional servers, clients, and other devices not shown. Intranet 102 is connected to ethernet 120, which is connected to ethernet 130 via firewall 125. Firewall 125 provides access to outside resources, such as servers 132, 134 and Internet 140, while protecting internal resources.

Internet 140 represents a worldwide collection of networks and gateways that use the transmission control

Docket No. AUS920000767US1

protocol/Internet protocol (TCP/IP) suite of protocols to communicate with one another. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers, consisting of thousands of commercial, government, educational and other computer systems that route data and messages. Of course, network data processing system 100 also may be implemented as a number of different types of networks, such as for example, an intranet, a local area network (LAN), or a wide area network (WAN). Figure 1 is intended as an example, and not as an architectural limitation for the present invention.

Firewall 125 also allows clients 108, 110, 112 to access servers 142, 144 via Internet 140. The firewall may reside on a server machine or may comprise a self contained firewall appliance, as known in the art. In accordance with a preferred embodiment of the present invention, document content is used to determine dynamic rules for IP address which should be inaccessible from an organization's computers. The firewall includes a rules table for filtering content. Keywords are entered into a search table. These keywords may include sexually related terms or other desired filter parameters. Incoming content not filtered by existing rules are scanned for the identified keywords. If such keywords are found, the originating IP address is added to the firewall rules table.

Referring to Figure 2, a block diagram of a data processing system that may be implemented as a server, such as servers 104, 132, 134, 142, 144 in Figure 1, is

Docket No. AUS920000767US1

depicted in accordance with a preferred embodiment of the present invention. Data processing system 200 may be a symmetric multiprocessor (SMP) system including a plurality of processors 202 and 204 connected to system bus 206. Alternatively, a single processor system may be employed. Also connected to system bus 206 is memory controller/cache 208, which provides an interface to local memory 209. I/O bus bridge 210 is connected to system bus 206 and provides an interface to I/O bus 212. Memory controller/cache 208 and I/O bus bridge 210 may be integrated as depicted.

Peripheral component interconnect (PCI) bus bridge 214 connected to I/O bus 212 provides an interface to PCI local bus 216. A number of modems may be connected to PCI bus 216. Typical PCI bus implementations will support four PCI expansion slots or add-in connectors. Communications links to network computers 108-112 in Figure 1 may be provided through modem 218 and network adapter 220 connected to PCI local bus 216 through add-in boards.

Additional PCI bus bridges 222 and 224 provide interfaces for additional PCI buses 226 and 228, from which additional modems or network adapters may be supported. In this manner, data processing system 200 allows connections to multiple network computers. A memory-mapped graphics adapter 230 and hard disk 232 may also be connected to I/O bus 212 as depicted, either directly or indirectly.

Those of ordinary skill in the art will appreciate that the hardware depicted in Figure 2 may vary. For

Docket No. AUS920000767US1

example, other peripheral devices, such as optical disk drives and the like, also may be used in addition to or in place of the hardware depicted. The depicted example is not meant to imply architectural limitations with respect to the present invention.

The data processing system depicted in Figure 2 may be, for example, an IBM RISC/System 6000 system, a product of International Business Machines Corporation in Armonk, New York, running the Advanced Interactive Executive (AIX) operating system.

With reference now to Figure 3, a block diagram illustrating a data processing system is depicted in which the present invention may be implemented. Data processing system 300 is an example of a client computer. Data processing system 300 employs a peripheral component interconnect (PCI) local bus architecture. Although the depicted example employs a PCI bus, other bus architectures such as Accelerated Graphics Port (AGP) and Industry Standard Architecture (ISA) may be used. Processor 302 and main memory 304 are connected to PCI local bus 306 through PCI bridge 308. PCI bridge 308 also may include an integrated memory controller and cache memory for processor 302. Additional connections to PCI local bus 306 may be made through direct component interconnection or through add-in boards. In the depicted example, local area network (LAN) adapter 310, SCSI host bus adapter 312, and expansion bus interface 314 are connected to PCI local bus 306 by direct component connection. In contrast, audio adapter 316, graphics adapter 318, and audio/video adapter 319 are connected to

PCI local bus 306 by add-in boards inserted into expansion slots. Expansion bus interface 314 provides a connection for a keyboard and mouse adapter 320, modem 322, and additional memory 324. Small computer system interface (SCSI) host bus adapter 312 provides a connection for hard disk drive 326, tape drive 328, and CD-ROM drive 330. Typical PCI local bus implementations will support three or four PCI expansion slots or add-in connectors.

An operating system runs on processor 302 and is used to coordinate and provide control of various components within data processing system 300 in Figure 3. The operating system may be a commercially available operating system, such as Windows 2000, which is available from Microsoft Corporation. An object oriented programming system such as Java may run in conjunction with the operating system and provide calls to the operating system from Java programs or applications executing on data processing system 300. "Java" is a trademark of Sun Microsystems, Inc. Instructions for the operating system, the object-oriented operating system, and applications or programs are located on storage devices, such as hard disk drive 326, and may be loaded into main memory 304 for execution by processor 302.

Those of ordinary skill in the art will appreciate that the hardware in Figure 3 may vary depending on the implementation. Other internal hardware or peripheral devices, such as flash ROM (or equivalent nonvolatile memory) or optical disk drives and the like, may be used in addition to or in place of the hardware depicted in Figure 3. Also, the processes of the present invention

may be applied to a multiprocessor data processing system.

The depicted example in **Figure 3** and above-described examples are not meant to imply architectural limitations. For example, data processing system 300 also may be a notebook computer or hand held computer in addition to taking the form of a PDA. Data processing system 300 also may be a kiosk or a Web appliance.

With respect to Figure 4, a block diagram of a
20 firewall host is depicted in accordance with a preferred
embodiment of the present invention. Firewall host 402
includes firewall rules table 420 and keyword search
table 430. When an site is identified as serving
inappropriate content, the IP address of the site is
25 added to firewall rules table 420. In the example shown
in Figure 4, the firewall rules table includes IPAddress1
422, IPAddress2 424, IPAddress3 426, and IPAddress4 428.
When a document request is received from inside the
firewall, the firewall host checks the IP address of the
30 site from which the document is being served. If the IP

Docket No. AUS920000767US1

address is in the firewall rules table, then the document access is blocked. U.S. Patent Application Serial No.

_____ (Attorney Docket No. AUS9-2000-0401-US1), which is hereby incorporated by reference, discloses a method and apparatus for building dynamic firewall rules based on content of downloaded documents. However, blocking an IP address based on whether keywords are found in one document might result in some sites being blocked unnecessarily and others. It would be advantageous to provide a more intelligent analysis of the source of documents, rather than a yes/no decision based on a single document.

In accordance with a preferred embodiment of the present invention, keyword search table 430 includes keywords 432 and corresponding point values 434. A sliding scale may be established for the severity and frequency of a possible filtered term. For example, a three point scale may award a term "sex" one point, because the term is deemed to be of low severity and is often used in place of the term "gender." The three point scale may also award one point to other terms having low severity, such as "sports" and "movies." However, the same three point scale may award a three point value to more severe terms, such as sexually graphic terms, obscenities, and terms suggesting violence or illegal activity.

The exemplary three point scale may also award two points to terms that are mildly inappropriate, such as religious or political terms, particularly concerning outgoing documents such as e-mail. While religious or political sites may not be considered inappropriate

09735539-11200

generally, a company may wish to prevent employees from expressing religious or political views using company resources, preferring for the employees to express these views on their own time and using their own resources.

An organizational policy may be established based upon three criteria. The first criteria is the number of points per document served (P_d) or the average number of points per document served from a given IP address (P_{davg}) relative to a threshold ($P_{dthresh}$). The number of points per document served is a total of the number of points for each keyword in the table (Kw_p). This is determined by comparing the document text with the keywords from the keyword search table.

The second criteria is the number of documents permitted before a decision is reached. This is called the decision interval (D_i). Alternatively, the decision may be determined as a length of time. The average

number of points per document (P_{davg}) may be computed over the decision interval and compared to the threshold (P_{dthresh}). In other words, P_{davg} is the sum of all the P_d divided by the number of documents received from the domain. If P_{davg} exceeds P_{dthresh} at the end of the decision interval, then the IP address of the site serving the documents is added to the firewall rules table.

The third criteria that may be considered for an organizational policy is a reset policy. The reset policy dictates what actions may be taken after the decision interval has been reached and the site is not deemed to be inappropriate. The reset policy may be that once D_i is reached with the threshold not exceeded, the site is automatically deemed to be "safe." However, the reset policy may dictate that the counter controlling the number of documents received is reset to zero and a new determination is made across the next D_i documents served. Alternatively, the reset policy may extend the decision interval into a moving window with a moving average based on the last D_i documents, such that a site will be evaluated upon every page served from it.

A person of ordinary skill in the art will realize that any of the above reset policies may be used within the scope of the invention. Furthermore, other reset policies may be devised. For example, the above policies may be used in combination based on a hierarchy of thresholds. Thus, if the average point value at the end of the decision interval is between zero and a first threshold the site is deemed to be safe; if the average point value is between the first threshold and a second threshold, the counter is reset to zero and the next Di

documents are considered; if the average point value is between the second threshold and a third threshold, the decision interval is extended into a moving window; and, if the average point value is higher than the third threshold, the IP address is added to the firewall rules table.

If an originating site is marked as a "known-safe" or "known-block" address, then documents from this address are not filtered again. This step is included to mitigate processing requirements upon the firewall computer. If a requested document originates from a "known-safe" source, then the document is simply passed through as requested.

Turning now to **Figure 5**, a flowchart is shown illustrating the operation of a content filtering process in accordance with a preferred embodiment of the present invention. The process begins and a determination is

made as to whether an exit condition exists (step 502). An exit condition may exist when the firewall host is shut down or filtering is deactivated. If an exit condition exists, the process ends.

10 If a request to access a document is received in
step 504, a determination is made as to whether the IP
address from which the document is served is in the
firewall rules table (step 506). If the IP address is in
the firewall rules table, the process blocks or permits
15 access to the document based on the rule (step 508) and
returns to step 502 to determine whether an exit
condition exists. For example, if the IP address is in
the firewall rules table as a "known-safe" source, then
access is permitted and if the IP address is in the
20 firewall rules table as a "known-block" source, then
access is blocked.

If the IP address is not in the firewall rules table in step 506, a determination is made as to whether it is the first document received from the domain (step 510).
25 If the document is the first document received from the IP address, the process sets the counter (d) to one (step 512) and calculates the point value (P_d) for the document (step 516). If the document is not the first document received from the domain in step 510, the process
30 increments the counter (step 514) and calculates the

point value (P_d) for the document (step 516). Next, a determination is made as to whether the decision interval is reached (step 518). If the decision interval is not reached, the process permits access (step 520) and returns to step 502 to determine whether an exit condition exists.

If the decision interval is reached in step 518, the process calculates the average point value (P_{avg}) for documents from the source (step 522). The average is calculated over the last D_i documents. Thus, if the counter is equal to D_i , then the average is the total of the P_d values for d being between 0 and D_i divided by D_i . If the counter is greater than D_i , then the average is a moving average, which is calculated each time through the process. Next, a determination is made as to whether the threshold (P_{thresh}) is exceeded (step 524). If the threshold is exceeded, the process adds the IP address to the firewall rules table as a "known-block" source and blocks access to the document (step 526). Then, the process returns to step 502 to determine whether an exit condition exists.

If the threshold is not exceeded in step 524, the process permits access (step 528) and resets the decision interval and manner in which the average is calculated (step 530). The step of resetting the decision interval may comprise declaring the source as "known-safe" and entering the IP address in the firewall rules table so that the site is not filtered again. The step of resetting the decision interval may comprise setting the counter (d) to zero. If the reset policy dictates that a

Docket No. AUS920000767US1

moving window is to be used, then the counter is allowed to exceed the decision interval and the average is computed over only the decision interval. Thereafter, the process returns to step 502 to determine whether an exit condition exists.

The present invention solves the disadvantages of the prior art by providing an intelligent and dynamic filtering mechanism at the firewall. This mechanism allows a company to maintain control over the use of client workstations. Viewing of pornography and other inappropriate subject matter can be governed within the workplace with a minimum of human interaction. Furthermore, by dynamically modifying filtering rules when such content is detected, the firewall may block on IP address, which is less computationally intensive than scanning all content when repeated requests are received for a site serving inappropriate content.

It is important to note that while the present invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium of instructions and a variety of forms and that the present invention applies equally regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media include recordable-type media such a floppy disc, a hard disk drive, a RAM, and CD-ROMs and transmission-type media such as digital and analog communications links.

The description of the present invention has been

0073589-1100

5
10

CONCLUSIONS